



**DEPARTMENT OF THE ARMY**  
**U.S. ARMY MANEUVER SUPPORT CENTER AND FORT LEONARD WOOD**  
**320 MANSCHEN LOOP STE 316**  
**FORT LEONARD WOOD, MISSOURI 65473-8929**

REPLY TO  
ATTENTION OF

31 OCT 2001

ATZT-IM

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy #41-01, Network Access, Internet Use and Internet Monitoring

1. PURPOSE. To establish policy for network access, internet use and monitoring of that use.

2. REASONS FOR POLICY:

a. To collect data for internet access and to ensure productivity during working hours.

b. To reduce the risk of viruses.

c. To improve network capacity planning.

d. To decrease network slowdown and keep productivity up.

e. To contain upgrade/expansion costs.

f. To prevent waste of Government resources.

g. To avoid any action that discredits the Army.

3. MISSION. The Directorate Of Information Management (DOIM) is the responsible agency for internet and network access. Effective operation of, and capacity planning for, our network and internet access are primary responsibilities of the DOIM. To effectively execute its responsibilities, the DOIM must monitor our network for maintenance, security and operational concerns IAW AR 380-19 and AR 380-53. Incidental to this monitoring the DOIM may discover unauthorized activities, as outlined in this policy. If such activities are discovered, they will be turned over to the unit commander/director, and if necessary, the proper investigative authorities for action.

4. POLICY/PROCEDURES. Every commander/director will ensure all personnel, with access to the network and internet, sign the enclosed usage policy. The activity's Information Systems Assurance Officer (ISSO) must be involved in this process. The DOIM will digitally maintain the signed copy. New personnel will not receive access to Fort Leonard Wood systems until they have attended the mandatory class and signed

ATZT-IM


SUBJECT: Command Policy #41-01, Network Access, Internet Use and Internet Monitoring

the agreement at the DOIM office when receiving their userid, certifying they understand the policy. Refusal to accept the attached agreement will result in limitation, denial or revocation of network access privileges.

5. Each activity will ensure all MANSCEN personnel with access to the network and internet understand the policy. This may be accomplished with awareness training by contacting DOIM for a one-hour optional class covering this policy.

6. PROPONENT. The proponent for this command policy is the DOIM, 563-6113.

Encl

  
WILLIAM A. VAN HORN  
Colonel, GS  
Chief of Staff

DISTRIBUTION:

All Brigades, Battalions, Companies,  
Detachments, Tenant Units, Directorates,  
Personal Staff Offices, and Contractors

## **FORT LEONARD WOOD ONLINE SYSTEMS USER AGREEMENT**

**PLEASE READ THIS AGREEMENT CAREFULLY. THIS AGREEMENT DESCRIBES THE BASIC RESPONSIBILITIES YOU ARE REQUIRED TO OBSERVE AS AN EMPLOYEE USING FORT LEONARD WOOD'S ONLINE SYSTEMS. THIS AGREEMENT STRIKES A FAIR BALANCE BETWEEN THE INSTALLATION'S INTERESTS AND YOUR NEEDS AND EXPECTATIONS. THIS AGREEMENT HAS BEEN MADE TO PROTECT BOTH YOU AND FORT LEONARD WOOD BY BEING AS CLEAR AND PRECISE AS POSSIBLE.**

THIS AGREEMENT, effective as of the date shown below, by and between Fort Leonard Wood and you, as a user of the installation's on-line systems

### **Section 1**

#### **USE OF FORT LEONARD WOOD'S ACCESS TO THE INTERNET**

- 1.1 Guidelines for Internet Access.** Access to the Internet increases our productivity and employee effectiveness, but it can become a time waster instead of a production enhancer if used without policy guidelines. The Army, not the user, is the owner of the Internet access provided over its network; therefore the Army has complete discretion over access privileges, nature of use, and content transmitted over its system, with the primary goal of making it a productive and stable environment. It must not be used in a manner which would waste resources or bring discredit on the Army. Internet access is provided by the Army for official business purposes to increase production and employee effectiveness only. To ensure the use of Internet access is done in a productive manner, a list of guidelines has been incorporated. All Fort Leonard Wood personnel are required to abide by the guidelines; any improper use of Government online systems is not acceptable and will not be permitted.

### **Section 2**

#### **ONLINE SYSTEMS POLICIES**

- 2.1 Monitoring Tools.** As the proponent for Internet access, the Directorate Of Information Management (DOIM) routinely monitors usage patterns of FLW's online communications. The reasons for monitoring are to maintain or increase online productivity, ensure enough access is available for official business, as well as for better planning and management of network resources.
- 2.2 Blocking of Internet Access.** Access to on-line systems is based on the nature of an employee's work. No access will be provided to employees having no official need for Internet access. Fort Leonard Wood reserves the absolute right to block Internet sites that violate this policy.

### **Section 3**

#### **OWNERSHIP OF ELECTRONIC COMMUNICATIONS**

- 3.1 All Communications Over the FLW Online Systems Are Property Of the Army.** Employees must not assume electronic communications are totally private. All messages created, sent, or retrieved over the FLW online systems are subject to disclosure by the Army, with or without advanced notice to the parties, for its own reasons, response to FOIA requests, litigation discovery, etc. The Army reserves the absolute right to access and monitor all messages and files on the FLW online systems.

*Orl*

## Section 4

### MAINTAINING A PROFESSIONAL AND HOSPITABLE ENVIRONMENT

- 1.1 **Public Image.** Army online systems are a place for business communications, and all communications over FLW online systems reflect our image. All employees are, therefore, responsible to maintain and enhance FLW's public image.
- 1.2 **EEO Concerns, Conduct, and Army Values.** Existing laws and Army policy address EEO concerns, personal conduct, and the Army Values. Use of Internet access must support these existing guidelines and laws. To ensure FLW online systems maintain a productive and stable environment, the following is not permitted: transmitting, retrieving or storing information that is discriminatory or harassing, obscene, pornographic or X-rated or reflects poorly on the Army; transmitting messages with derogatory or inflammatory remarks about a person's race, color, sex, age, disability, religion, national origin, physical attributes and sexual preference; using the FLW online systems for personal gain or any other purpose, which is illegal, or against Army policy or contrary to the Army's best interest.
- 1.3 **Employee's Identity.** No message can be transmitted without the employee's identity. Transmittal of messages using another employee's access or anonymous or fictitious names is prohibited

## Section 5

### CONFIDENTIALITY

- 5.1 **Communication of Messages Disclosing Classified or Sensitive Information.** You recognize that your position with the Army requires considerable responsibility and trust. Relying on your ethical responsibility and undivided loyalty, the Army may entrust you with highly sensitive or classified information. You are legally and ethically responsible for protecting this information. No messages disclosing sensitive, restricted, non-public, proprietary, Privacy Act-protected, or procurement-sensitive information, for other than official purposes, may be transmitted over the FLW online systems. The general access FLW online system is not a secure means of transmitting classified information and will not be used for that purpose.

## Section 6

### MAINTAINING SYSTEM SECURITY

- 6.1 **Keeping the Online System Secure from Computer Viruses.** To prevent viruses from entering the FLW and Army online systems, antivirus software must be loaded and activated on all PCs accessing the system. Any viruses detected must be reported to your unit ISSO immediately. If your ISSO is not available report the incident to OIS. They will contact the DOIM as needed.

## Section 7

### COPYRIGHT

- 7.1 **Copyright Infringement.** No copying, downloading, or distributing of any of the registered copyrighted materials including but not limited to messages, e-mail, text files, program files, image files, database files, sound files and music files, beyond the terms of licenses, limited rights, or permitted uses allowed by the copyright holder, through the FLW online systems is allowed. Personal software will not be copied to any Army computer, without authorization from the DOIM.

## Section 8

### PERSONAL USE

**8.1 Prohibited Personal Use.** The following personal uses of the Internet are prohibited since they take valuable bandwidth or violate other provisions of this policy:

- a. Chat Room programs; e.g. those offered by ICQ, AOL, Excite, Yahoo, etc.
- b. Instant/Immediate Messaging
- c. Pager programs
- d. On-line Selling, i.e. auction houses like Ebay or stocks from Fidelity
- e. News Streamers
- f. Checking personal Email accounts, i.e. HotMail
- g. On-line gaming

**8.2 Limited Personal Use.** FLW network resources, including those used to gain access to Internet-based sites, are only to used for the express purpose of performing work-related duties. Supervisors may approve the network resources beyond the scope of this limited access policy when said use meets the following conditions:

- a. The intended use of network resources is incidental
- b. The intended use of network resources does not interfere with the employees regular duties
- c. The intended use of network resources is for educational purposes and within the scope of the employee's job function
- d. The intended use of network resources does not break any local, state, or federal laws.
- e. The intended use of network resources will not overburden the network

## Section 9

### VIOLATIONS

**9.1 Failure to Comply.** DOIM will notify an employee's/soldier's Commander/Director for failure to comply with this policy. Civilian employees failing to comply with this policy will face a range of disciplinary actions up to and including termination. Military personnel are subject to UCMJ action. Contractors, not adhering to this policy will face the loss of access to the systems. For serious violations, more strenuous actions will be pursued with the contractor employee's supervisory chain.

#### ACCEPTED:

As a civilian/contractor/military member of Fort Leonard Wood, I have received a copy of the installation's Policy Guidelines on access to the Internet system. I hereby accept and agree to abide by the standards set in the Policy for the duration of my employment on Fort Leonard Wood.

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

Employee's Printed Name: \_\_\_\_\_

\_\_\_\_\_  
Unit ISSO Signature:

\_\_\_\_\_  
Date

Unit Information Systems Security Officer (ISSO) Printed Name: \_\_\_\_\_